UNIVERSIDADE DA CORUÑA

TRABAJO FIN DE MÁSTER UNIVERSITARIO EN ABOGACÍA
Curso 2019-2020

ADAPTACIÓN DE UNA ENTIDAD LOCAL A LA NUEVA NORMATIVA EN PROTECCIÓN DE DATOS.

ADAPTACIÓN DUNHA ENTIDADE LOCAL Á NOVA NORMATIVA EN PROTECCIÓN DE DATOS

Adaptation of a local entity to the new data protection regulation

Autora: Manuela Lorenzo Rodríguez
Tutor: Gonzalo Barrio García

ÍNDICE DE CONTENIDOS

LISTADO DE ABREVIATURAS Y SIGLAS

APDCAT: Autoridad catalana de Protección de datos

AEPD: Agencia Española de Protección de Datos

DPD: Delegado de Protección de datos

EIPD: Evaluación de impacto en protección de datos

ET: Encargado del Tratamiento

GT29: Grupo de Trabajo sobre Protección de Datos del artículo 29

LCSP: Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

LPACAP: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

LBRL: Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local

RAT: Registro de Actividades de Tratamiento

ROF: Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales

RGPD: REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

TREBEP: Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público

I.- INTRODUCCIÓN

1.- Motivación y objetivos

En este primer apartado quiero manifestar los motivos que me han llevado a la realización del presente trabajo de fin de máster y las razones que me han movido a la elección de la protección de datos como objeto de estudio.

En el último año he venido desarrollando mi actividad profesional en el ámbito de la protección de datos en la Diputación Provincial de A Coruña, dependiendo directamente de la delegada de protección de datos de la citada administración .

Esto me ha permitido profundizar en múltiples aspectos relacionados con esta materia, desde los más generales a los más específicos, al intentar introducir en la documentacion y el "*modus operandi*" de la Diputación de A Coruña, las novedades y requisitos que han ido surgiendo en los últimos años y que ha ido desarrollando la nueva normativa en materia de protección de datos.

Todas estas circunstancias me han supuesto una motivación y un reto muy importante, al permitirme profundizar en aspectos en los que mi formación anterior estaba poco sedimentada. Sin embargo, en el desarrollo de mi actividad profesional me he topado con diferentes barreras, derivadas principalmente de la falta de jurisprudencia dada la reciente entrada en vigor de la nueva normativa y de las abundantes interpretaciones doctrinales contradictorias.

Por lo expuesto, debido a que existe una limitada jurisprudencia actualizada, en este trabajo se citan determinadas sentencias anteriores a la nueva normativa, que no contradicen lo establecido en la misma.

En segundo lugar, voy a justificar las razones de la elección del ámbito de la protección de datos desde un punto de vista técnico. La motivación surge a partir de la entrada en vigor del nuevo Reglamento de Protección de Datos a nivel europeo y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales a nivel estatal y de su aplicación directa a las entidades locales.

Para conocer y aplicar las novedades establecidas en la citada normativa, se requiere profundizar sobre los nuevos requisitos y los posibles conflictos con otra normativa como por ejemplo la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Si bien es cierto que la Agencia Española de Protección de Datos ha publicado diferentes guías, las cuales se citan a lo largo de este trabajo, muchas veces la problemática con la que nos topamos diariamente en las entidades locales, no se encuentra reflejada en las recomendaciones publicadas.

Además, existe limitada bibliografía actualizada, por lo que los trabajadores de las entidades locales en el ámbito de la protección de datos nos vemos abocados a realizar una interpretación propia de las diferentes interpretaciones doctrinales disponibles para consulta.

Es por ello que este trabajo está orientado a la realización de una implantación práctica de la nueva normativa de protección de datos en el ámbito de las entidades locales, teniendo en cuenta aquellas particularidades que he ido conociendo a lo largo de mi experiencia profesional en el campo.

2.- Estructura

Este Trabajo Fin de Máster está estructurado en los siguientes puntos:

I. Una breve introducción del trabajo desarrollado la motivación, los objetivos y la estructura del presente trabajo.

II. Una introducción al régimen jurídico de aplicación y el desarrollo del nuevo concepto de "Responsabilidad Proactiva" con delimitación de las diferentes figuras implicadas en la responsabilidad en el tratamiento de datos personales.

III. Explicación de las siguientes medidas de obligada adopción: Nombramiento del delegado de protección de datos en las entidades locales y el nuevo Registro de Actividades de Tratamiento.

IV. Se estudiarán las consecuencias prácticas de la implantación de las medidas establecidas en la nueva normativa referidas al derecho de información de las personas interesadas.

V. En esta etapa se va a explicar la configuración del nuevo consentimiento y la problemática derivada del consentimiento de los menores de edad.

VI. Se va a estudiar la situación de la aplicación de la normativa en el ejercicio de los derechos de protección de datos.

VII. Se tratan las implicaciones existentes en las diferentes identificaciones de las personas interesadas que pueden llevar a cabo las entidades locales.

VIII. Estudio sobre las modificaciones de la normativa de contratación pública en relación coa la protección de datos personales y la problemática diferenciación entre encargados y corresponsables del tratamiento de datos personales.

IX. Análisis de la gestión de riesgos a llevar a cabo por las entidades locales, incluyendo el análisis de riesgos, las evaluaciones de impacto y la gestión de una posible brecha de seguridad

X. Se trata la confrontación existente entre la protección de datos personales y el deber de transparencia que pesa sobre las entidades locales.

XI . Conclusiones

II.- DELIMITACIÓN RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS Y PRINCIPIO DE RESPONSABILIDAD PROACTIVA

1.- Encuadre constitucional

El derecho a la protección de datos se configura como el derecho fundamental que permite a cualquier persona controlar el uso que se hace de sus datos personales y decidir sobre los mismos.

En nuestro país, podemos entender que el derecho fundamental a la protección de datos deriva del artículo 18.4 de la Constitución que establece que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

Se debe a la labor tuitiva del Tribunal Constitucional en materia de derechos fundamentales y libertades públicas, el alumbramiento de un nuevo derecho fundamental *ex* art. 18.3 CE.

La STC núm. 254/1993 , delimita el derecho fundamental a la protección de datos o "*habeas data*" en su fundamento jurídico séptimo:

> *"Un primer elemento, el más «elemental», de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: El uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos . Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)"*

El "*habeas data*" constituye un Derecho Humano Fundamental de cuarta generación, fuertemente vinculado a la creciente globalización, al rápido avance de nuevas tecnologías y la democratización en el acceso a la información. Se encuentra definido en el Diccionario de español jurídico como aquella "*Acción constitucional que puede ejercer cualquier persona incluida en un registro de datos para acceder al mismo y recabar la información que le afecte, así como para solicitar su eliminación o corrección si tal información fuera falsa o estuvera desactualizada*".

La STC núm. 292/2000, de 30 de noviembre, aclara el alcance y el contenido del derecho a la intimidad en su fundamento jurídico sexto:

> *"Dispone el art. 18.4 C.E. que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una nueva garantía*

constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

La Sentencia núm. 366/2015 de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª) de 27 de octubre, explica de manera muy clara cual es el objeto completo del derecho a la protección de datos:

"El derecho a la protección de datos tiene, por tanto, un objeto más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art 18.1 CE , sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inseparablemente unidos al respeto de la dignidad personal, como el derecho al honor, y al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales -como aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo-, porque su objeto no es sólo la intimidad individual, protegida ya por el art 18.1 CE, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

En relación con su contenido, el derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho a la intimidad, con el objeto de garantizar a la persona un poder de control sobre sus datos personales. Entre ellos, destacan el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. De este modo se garantiza el poder de disposición sobre los datos personales.

Por lo que atañe al derecho a la libertad de expresión, a la luz de la doctrina del Tribunal Constitucional, de la que son exponente sus sentencias 23/2010 ,de 27 de abril , y 9/2007, de 15 de enero , ha de señalarse que, consagrado en el artículo 20 de la Constitución , comprende, junto a la mera expresión de pensamientos, creencias, ideas, opiniones y juicios de valor, la crítica de la conducta de otro, aun cuando la misma sea desabrida y pueda molestar, inquietar o disgustar a quien se dirige, pues así lo requieren el pluralismo, la tolerancia y el espíritu de apertura, sin los cuales no existe sociedad democrática.

2.- Encuadre normativo

El 25 de Mayo de 2016 entró en vigor el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD).

Los reglamentos europeos tienen aplicación directa, sin embargo, cuando es necesario adaptar la normativa estatal para adaptarla al nuevo marco regulatorio de la Unión Europea se puede considerar que es preciso un desarrollo normativo. De este modo, la modificación europea hacía imprescindible la reforma de la regulación de la protección de datos en España.

Dicha reforma normativa se llevo a cabo con la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), que se aprueba para adaptarse al RGDP. Según se lee en el punto III del preámbulo:

"La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica."

La Ley Orgánica incluye nuevo contenido[1], sin embargo, hay determinadas previsiones de la derogada LO 15/1999 que permanecen vigentes:

1 Nuevo contenido: los principios y derechos en protección de datos (arts. 4 y ss.); la regulación de concretos tratamientos (arts. 19 y ss.); la ampliación de funciones del delegado de protección de datos (art.37); el régimen de la Agencia de Protección de Datos estatal y de las autonómicas (arts. 44 y ss.); el procedimiento ante vulneraciones (arts. 63 y ss.) y el régimen sancionador (arts. 70 y ss.); los citados derechos digitales (arts. 69 y ss.); y doce reformas legales (en disposiciones finales, sobre régimen electoral, Poder Judicial, sanidad, jurisdicción contencioso-administrativa, enjuiciamiento civil, universidades, autonomía del paciente, educación, transparencia, procedimiento administrativo, Estatuto de los Trabajadores, y empleo público).

- El artículo 23.1 de la LO 15/1999 que se refiere a las denegaciones al ejercicio de los derechos de acceso, rectificación y cancelación por razones de defensa del Estado o seguridad pública, o por las necesidades de investigación o protección de derecho de terceros.
- El artículo 23.2 que alude a esa denegación del ejercicio de derechos por parte de los responsables de los ficheros de la Hacienda Pública en caso de que supongan un obstáculo para las actuaciones administrativas «tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras».
- El artículo 24 regula las excepciones al derecho de información cuando «afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales».
-Además la disposición transitoria transitoria cuarta supone la continuación de vigencia del artículo 22 (relativo a los antiguos ficheros de las Fuerzas y Cuerpos de Seguridad del Estado), mientras España no transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

3.- El principio de responsabilidad proactiva

Una vez delimitado el régimen jurídico aplicable, procede abordar las novedades que presenta la nueva normativa en protección de datos. La mayor novedad que presenta el RGPD es la evolución de un modelo basado, fundamentalmente, en el control de cumplimiento, en otro que descansa en el principio de responsabilidad proactiva.

Tal y como lo describe la AEPD[2] "*El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la norma.*
En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.
En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.
Además, el RGPD adopta un enfoque proactivo, exigiendo que el responsable adopte medidas preventivas dirigidas a reducir los riesgos de incumplimiento y, además, que esté en condiciones de demostrar que ha implantado esas medidas y que las mismas son las adecuadas para lograr la finalidad perseguida"

En este mismo sentido, el considerando 78 del RGPD establece lo siguiente:

2 AEPD "Responsabilidad proactiva" Disponible en: https://www.aepd.es/reglamento/cumplimiento/principio responsabilidad-proactiva.html

"*La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto*"

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

ACÍN FERRER[3] establece que **"***supone que tanto el responsable como el encargado del tratamiento han de valorar detalladamente los riesgos de incumplimiento de la normativa, resultantes de la gestión diaria del tratamiento de datos personales que son propios de su actividad y deben adoptar las medidas que procedan, asegurando su capacidad para demostrar tales actuaciones preventivas*".

A. El responsable individual del tratamiento de datos personales

Es de vital importancia, en la medida que el reglamento asigna la obligación al responsable del tratamiento de protección de datos de llevar a cabo medidas de seguridad y lo hace directamente responsable de las mismas, la definición de esta figura.

La normativa define al responsable de tratamiento RGPD como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Esta definición establece que podrá ser responsable de tratamiento toda aquella empresa, organismo o individuo que trate datos de carácter personal bajo su nombre, es decir, que decida voluntariamente llevar a cabo un tratamiento de datos de carácter personal, recogidos en un fichero del que es titular y tomando decisiones sustanciales sobre cómo tratar los datos y los fines que ser persiguen con el mismo.

3 ACÍN FERRER, A. (2019) *Protección de datos. Aplicación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, en las entidades locales Entidades locales.- Actuaciones y responsabilidades.* La Administración Práctica num. 2/2019.

Según la AEPD[4] *"En el ámbito de la Administración Local, el responsable del tratamiento, considerando la normativa de régimen local aplicable, recaerá en los municipios, diputaciones provinciales e islas. No obstante, sobre estas últimas procede realizar la siguiente consideración: Las diputaciones provinciales, consejos y cabildos insulares, serán responsables de sus respectivos tratamientos, es decir, sobre aquellos sobre los que decidan los fines de los mismos y respecto a aquellos tratamientos de datos derivados de la prestación de asistencia en favor de los municipios, serán encargados de tratamiento."*

B. La corresponsabilidad en el tratamiento de datos personales

A mayores de lo establecido por la AEPD en la Guía Protección de Datos y Administración local, referido en el punto anterior, debemos considerar respecto de las Entidades Locales la posibilidad de que actúen como corresponsables de sus respectivos tratamientos junto con otro responsable, tal y como establece el RGPD en su artículo 26:

> *"Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento."*

El nuevo Reglamento europeo, en el artículo 26, crea esta nueva figura inexistente en la LOPD, los Corresponsables del tratamiento, para cuando se determinan conjuntamente entre varios Responsables los fines o los medios del tratamiento.

III.- MEDIDAS DE OBLIGADA ADOPCIÓN

1.- Nombramiento del delegado de protección de datos

El artículo 37 del RGPD establece lo siguiente:

> *1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*
>
> *a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial*

CAMPOS ACUÑA[5], desarrollando el concepto de DPD en el ámbito local, viene a proporcionar definición en los siguientes términos "*El RGPD regula la figura del Delegado de Protección de Datos (DPD) en los artículos 37 a 39, sin perjuicio de que aparece mencionado en otras partes del articulado, así como en los considerandos de la norma. Según el RGPD (artículo 37.5 y considerando 97), el DPD será una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos y con capacidad para desempeñar las funciones que el*

4 Guía "*Protección de datos y Administración Local*". AEPD, 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

5 CAMPOS ACUÑA, C. (2018), *Aplicación práctica y adaptación de la protección de datos al ámbito local*, 2ª edición, Madrid. N.º de página: 389.

RGPD le atribuye. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos". RALLO LOMBARTE[6] aborda la cuestión y afirma que el DPD constituye "*una figura preexistente aunque no reconocida*".

LÓPEZ CALVO[7] considera que "*el DPD es responsable de asegurar el cumplimiento del Reglamento y de la normativa nacional sobre la materia*".

A. Contratación

El artículo 37.6 del RGPD establece que "*El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios"*.

La contratación externa de la figura del delegado de protección de datos en el ámbito de las Administraciones Públicas es un tema ampliamente discutido. El contrato de servicios es objeto de regulación en el artículo 17 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público que establece que "S*on contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o suministro, incluyendo aquellos en que el adjudicatario se obligue a ejecutar el servicio de forma sucesiva y por precio unitario. No podrán ser objeto de estos contratos los servicios que impliquen ejercicio de la autoridad inherente a los poderes públicos"*

Lo mismo establece la Junta Consultiva de Contratación administrativa en su informe 52/2009 de 26 de febrero de 2010, afirmando que no pueden ser objeto de un contrato de servicios los que impliquen ejercicio de la autoridad inherente a los poderes públicos y también que la razón de ser de esta razón es evidente: la reserva a los funcionarios públicos del "ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de las potestades públicas o en la salvaguardia de los intereses generales del Estado y de las Administraciones Públicas"

La AEPD, establece que "*El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.*

6 RALLO LOMBARTE, A. (Dtor.) (2019), *Tratado de Protección de Datos, actualizado con la Ley Orgánica 3/2018, de 5 de diciembre.* 1º edición, Valencia. N.º de página: 431

7 LÓPEZ CALVO, J. (Coord.) (2018)*, El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* 1ª edición, Madrid, BOSHH – Wolster Kluver, pág 493

La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.
La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran:

- *total autonomía en el ejercicio de sus funciones*
- *necesidad de que se relacione con el nivel superior de la dirección*
- *obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad*

B. Comunicación del nombramiento a la AEPD

Conforme al artículo 37.7 RGPD, "*El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control".* Más concretamente, el artículo 34.3 y 4 LOPDGDD establece un plazo de 10 días para *"Comunicar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria".*

La Guía rápida de comunicación del Delegado de Protección de Datos[8] publicada por la AEPD establece las directrices para llevar a cabo la notificación a la Autoridad de Control.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

2.- Registro de actividades del tratamiento (RAT)

Una de las novedades más importantes en el cumplimiento de las obligaciones en materia de protección de datos es la desaparición de la obligación de notificar los ficheros o tratamientos con datos personales a la AEPD, siendo sustituida por la obligación de mantener un Registro de Actividades de Tratamiento actualizado y accesible por medios electrónicos.

A. Sujetos obligados

El artículo 31.1 de la LOPDGDD establece que "*Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5"* y en su apartado segundo establece que, los sujetos enumerados en el artículo 77.1, entre los que se encuentran las administraciones públicas, "*harán público un*

8 "GUÍA RÁPIDA DE COMUNICACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS". AEPD, 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-rapida-dpd.pdf

inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal."

Por lo tanto, los responsables y encargados de tratamientos de la Administración local deben mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico, que estará a disposición de la Autoridad de Control, en el que se incluya una descripción de los tratamientos de datos que realicen.

B. Contenido

El registro como responsables del tratamiento deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos
b) los fines del tratamiento
c) una descripción de las categorías de interesados y de las categorías de datos personales
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias transfonterizas, la documentación de garantías adecuadas
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

El registro como encargados del tratamiento deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del encargado, del representante del encargado, y del delegado de protección de datos
b) categoría de tratamientos efectuados por cuenta de cada responsable
c) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias transfonterizas, la documentación de garantías adecuadas
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

IV.- AMPLIACIÓN DEL DERECHO A LA INFORMACIÓN

El derecho a la información se regula, en los artículos 13 y 14 RGPD, así como en los considerandos 60 a 62 RGPD, que se transcriben a continuación:

"(60) *Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente*

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas."

La obligación de informar a los interesados sobre las circunstancias relativas al tratamiento de sus datos personales, recae sobre el responsable del tratamiento. El RGPD añade información adicional a la que hasta ahora exigía la antigua LOPD, y distingue la información que deberá facilitarse cuando los datos personales se obtengan del interesado y cuando los datos personales no se hayan obtenido directamente del interesado.

Además existen diferencias tanto en cuanto a la información a facilitar, como en relación al momento en el que hay que cumplir con esta obligación.

El artículo 13 RGPD amplía la información que ha de facilitarse al interesado cuando se han obtenido los datos personales de él directamente. Esta información la podríamos clasificar en:

a) Aquella información que siempre deberá facilitarse al interesado:

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- La finalidad del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
- La posibilidad de revocar el consentimiento prestado.
- El derecho a presentar una reclamación ante una autoridad de control.

b) Aquella otra información que varía en función de que la misma sea aplicable al supuesto de hecho, o al concreto responsable de tratamiento de que se trate. Así, en el caso de un tratamiento llevado a cabo por una entidad local la información a facilitar al interesado sería:

- Los datos de contacto del Delegado de Protección de Datos
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso
- La intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión.
- De la existencia de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.
- La existencia de comunicaciones de datos, bien por requisito legal o contractual, y de la obligación a facilitar dichos datos y las consecuencias de la negativa a facilitarlos.

Por otra parte, cuando los datos no hayan sido recabados u obtenidos del interesado, según el artículo 14 RGPD, el responsable deberá facilitar, además de la información anterior, información al respecto del origen de los datos y de las categorías de datos tratados.

La AEPD señala para el cumplimiento del deber de informar[9] que "*para hacer compatible la mayor exigencia de información que introduce el RGPD, la concisión y comprensión en la forma de presentarla, se recomienda adoptar un modelo de información por capas o niveles, dividiendo la información en dos capas"*

- Primera capa con la información básica, de forma resumida, en el mismo momento y medio en que se recojan datos.
- Segunda capa con la información adicional preceptiva, de forma más detallada.

La forma de presentación preferente de la primera capa debería de ser (según recomienda la AEPD en su Guía) en forma de tabla, garantizando que dicha información quede dentro del «campo de visión» del interesado, según sea el medio utilizado en la recogida de la información.

9 "Guía para el cumplimiento del deber de informar". AEPD, 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

En las entidades locales se emplean formas muy diferentes para la recogida de los datos y por ello es necesario adaptar todas ellas a la nueva normativa.

1.- Adaptación de formularios en papel

En el caso de los formularios en papel puede no ser recomendable utilizar el modelo por capas ya que la segunda capa cambia en función de cada tratamiento específico y tener un archivo con todas las segundas capas de cada uno de los tratamientos llevados a cabo por la entidad local es ineficaz y resulta más cómodo y lógico facilitar toda la información requerida por la normativa en el formulario que recoja cualquier tipo de datos.

Es necesario tener en cuenta que en algunos casos se requerirá el consentimiento expreso para el tratamiento de los datos personales contenidos en el formulario y en otros caso solamente se debe informar, cuando la base legitimadora sea otra diferente al consentimiento.

Un ejemplo de un cuadro de información adecuado a la nueva normativa es el siguiente:

Responsable	Datos de contacto del responsable
	Datos de contacto del Delegado de Protección de Datos
Corresponsable	Datos de contacto del corresponsable (si existe)
Encargado	Datos de contacto del encargado del tratamiento (si existe)
Finalidad	Descripción ampliada de los fines del tratamiento
	Plazos o criterios de conservación de los datos
	Decisiones automatizadas, perfiles y lógica aplicada
Base legitimadora	Detalle de la base jurídica del tratamiento
	Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios	Destinatarios o categorías de destinatarios
	Previsión de transferencias internacionales
Derechos	Derechos y formar de ejercicio
	Derecho a retirar el consentimiento y consecuencias
	Derecho a reclamar ante la AEPD

2.- Adaptación de formularios web

En los formularios web es muy recomendable utilizar el modelo en dos capas que recomienda la AEPD, ya que facilitar toda la información requerida en una primera capa no permite que esté en el campo de visión del interesado normalmente.

De acuerdo con el artículo 11.1 de la nueva LOPDGDD, en el caso de que se recogieran los datos a través de redes de comunicaciones electrónicas o en el marco de la prestación de un servicio de la sociedad de la información (a nuestros efectos y como ejemplo, un formulario electrónico o telemático), así como en aquellos otros supuestos expresamente establecidos por la ley o cuando así lo autorice la Agencia Española de Protección de Datos, «*el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información*».

Tal y como establece la Guía del deber de informar[10] "*en un formulario de solicitud, la tabla con la información básica debería situarse en el mismo campo de visión que el lugar donde haya de manifestarse la conformidad con lo solicitado (el botón de "enviar", si es un formulario electrónico), formando parte de la copia que quede a disposición del interesado".*

Un ejemplo de cuadro de información a incluir en la primera capa, siguiendo lo establecido en el artículo 11 de la LOPDGDD es el siguiente:

Responsable	Datos de contacto del responsable
Finalidad	Descripción fines del tratamiento
Derechos	Derechos y forma de ejercicio
Información adicional	Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles
	Enlace a la 2ª capa de la información donde conste toda la información restante obligatoria

Un ejemplo de cuadro de información a incluir en la segunda capa es el siguiente:

Responsable	Datos de contacto del responsable y del representante en su caso
	Datos de contacto del delegado de protección de datos
Finalidad	Descripción ampliada de los fines del tratamiento
	Plazos o criterios de conservación de los datos
	Decisiones automatizadas, perfiles y lógica aplicada
Legitimación	Detalle de la base legitimadora
	Obligación de facilitar o no los datos y consecuencias de no hacerlo
Destinatarios	Destinatarios
	Transferencias internacionales

10 "Guía para el cumplimiento del deber de informar". AEPD, 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

Derechos	Derechos y forma de ejercicio
	Derecho a retirar el consentimiento
	Derecho a reclamar ante la Autoridad de Control

El enlace a la 2ª capa de la información deberá ser individualizado respecto de cada tratamiento de datos personales. Es decir, no es correcto enlazar con la política de privacidad de la entidad local o con su RAT si este no establece separadamente y con suficiente precisión toda la información a facilitar en la 2ª capa referente al tratamiento específico.

Es necesario diferenciar aquellos tratamientos en los que la base legitimadora sea el consentimiento del interesado, ya que este deberá ser expreso y por lo tanto en un formulario web lo correcto sería incluir una casilla no pre-marcada para que la persona afectada consienta expresamente.

3.- Especialidades del derecho a la información en los tratamientos con fines de videovigilancia

Tal y como establece el artículo 22.4 de la LOPDGDD, en referencia a los tratamientos con fines de videovigilancia *"El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento"*

Un ejemplo de cuadro de información a incluir en el dispositivo informativo es el siguiente:

Responsable del tratamiento
Finalidad del tratamiento
Derechos y forma de ejercerlos
Forma de acceso a la restante información

Normalmente las entidades locales no gestionan directamente la videovigilancia de sus instalaciones, sino que es una empresa con un contrato de servicios quien lo gestiona como encargada del tratamiento. Sin embargo, el responsable del tratamiento sigue siendo la entidad local contratante por lo que los datos a incorporar en el dispositivo informativo serán los establecidos por la entidad local, que deberán figurar en las cláusulas del contrato junto con aquellas otras obligaciones derivadas de un "encargo" de tratamiento.

Es habitual encontrar resoluciones de la AEPD que sancionan a Entidades Locales con apercibimientos por la colocación de dispositivos de video-vigilancia sin informar debidamente a la ciudadanía.

Por ejemplo, en la resolución núm. *R/00224/2019*, la AEPD apercibe al Ayuntamiento de Coria del Rio por infracción del artículo 6 RGPD, tipificada en el art. 83.5 letra a) RGPD, al haber instalado un dispositivo de video-vigilancia con afectación al derecho de terceros sin causa justificada, siendo la misma sancionada en virtud de lo dispuesto en el artículo 58.2 RGPD y requerida para el cumplimiento de las siguientes medidas: Aportación de impresión de pantalla (fecha y hora) de lo que en su caso se capta con el dispositivo en cuestión, aportación de prueba fotográfica del cartel informativo, indicando expresamente el responsable ante el que se pueda ejercitar los derechos reconocidos en la Legislación vigente y explicación motivada de la causa/motivo de la instalación de la cámara en cuestión.

V.- CONSENTIMIENTO

1.- Cambios en el consentimiento

El RGPD introduce como novedad, la modificación de la forma en la que deberá recabarse el consentimiento del interesado.
Se redefine el concepto de consentimiento del interesado como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

El RGPD adiciona un requisito formal para la obtención del consentimiento y así garantizar que sea inequívoco: el consentimiento deberá ser recabado mediante una declaración o mediante una clara acción afirmativa.

A. Consentimiento explícito

El RGPD establece los supuestos en los que el consentimiento además de ser inequívoco, deberá ser explícito:

- Cuando se haga tratamiento de categorías especiales de datos personales (artículo 9.2.a RGPD)
- Cuando se adopten decisiones automatizadas y elaboración de perfiles (artículo 22.2.c RGPD)
- Cuando se realicen transferencias internacionales (artículo 49.1.a RGPD)

En estos casos, el interesado deberá aceptar el tratamiento de sus datos personales por medio de una declaración por escrito, medios electrónicos, declaración verbal o marcando una casilla de un sitio web de Internet en la que se manifiesta que acepta las condiciones del tratamiento.

2.- La problemática del consentimiento de los menores entre 14-18 años

La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil matiza algunos de los derechos contenidos en los Tratados Internacionales de los que España es parte , combinando, por una parte, la posibilidad de su ejercicio con la necesaria protección que, por razón de la edad, los menores merecen.
La citada Ley y sus disposiciones de desarrollo son de aplicación a los menores de dieciocho años que se encuentren en territorio español, salvo que en virtud de la ley que les sea aplicable hayan alcanzado anteriormente la mayoría de edad.

El artículo 8 RGPD prevé, bajo el nombre de Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información que:

> *"1. Cuando se aplique el art.6, aptdo 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.*
> *Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años."*

Sin embargo, no parece que la voluntad del legislador europeo fuera la de excluir la aplicación del reglamento a las muchas otras situaciones de consentimiento de menores que no se circunscriban exclusivamente a los servicios de la sociedad de la información, ya que encontramos menciones a los menores de edad a lo largo de todo el texto del Reglamento, referencias que otorgan siempre al tratamiento de sus datos una especial protección y consideración.

Hasta la entrada en vigor de la LOPDPGDD la cuestión estuvo regulada en el art. 13 del Real Decreto 1720/2007[11], de 21 de diciembre, que consideraba que «*los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal*».

En el trámite de enmiendas en el Congreso, el texto de la LOPDPGDD sufrió varios cambios; el entonces Proyecto de ley cambió el texto en lo que se refiere a la edad de consentimiento.
Antes de someterse al trámite de enmiendas el art.7 fijaba en trece años la edad para prestar consentimiento. Sin embargo, aceptando la enmienda propuesta por el Partido Socialista, el texto publicado en el Boletín Oficial de las Cortes Generales el 26 de octubre de 2018 establece lo siguiente:

11 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.
Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.
2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.»

VI.- EJERCICIO DE LOS DERECHOS DE PROTECCIÓN DE DATOS

1.- Características de los derechos

Conforme a la nueva normativa los derechos que el interesado tiene en materia de protección de datos son: derecho de acceso, rectificación, supresión (el derecho al olvido), a la limitación del tratamiento, a la portabilidad de los datos, de oposición y a no ser objeto de decisiones individuales automatizadas.

Según la AEPD[12] estos derechos se caracterizan por lo siguiente:

- Su ejercicio es gratuito
- Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá cobrar un canon proporcional a los costes administrativos soportado o negarse a actuar
- Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más
- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que opte por otro medio
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control
- Puedes ejercer los derechos directamente o por medio de tu representante legal o voluntario
- Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule

2.- Ejercicio de los derechos de protección de datos

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, obliga al responsable del tratamiento "a *informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente*

12 AEPD "Ejerce tus derechos" Disponible en: https://www.aepd.es/reglamento/derechos/index.html

accesibles para el afectado" por lo que es recomendable facilitar un formulario en el que conste toda la información referente a los derechos y las instrucciones para el envío del mismo.

En dicho formulario deberá figurar:

- El tratamiento sobre el que se ejercita el derecho
- Datos de contacto de la persona presentadora de la solicitud
- Datos, en su caso, de la persona representada
- Derechos que se ejercitan
- Información adicional sobre el derecho que se ejercita
- Documentación que se acompaña

El derecho de acceso, permite al presentador solicitar confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, que se le facilite la información relacionada en el artículo 15 del RGPD. En cambio con el derecho de rectificación el presentador solicita que se rectifiquen los datos personales inexactos que le conciernan o se completen aquellos que sean incompletos.
Al ejercer el derecho de supresión el presentador solicita que se supriman sin dilación indebida los datos personales y mediante el derecho a la limitación al tratamiento el presentador solicita que se limite el uso de sus datos personales. Sin embargo, al ejercer el derecho de oposición el presentador se opone a que los datos personales que le conciernan sean objeto de un tratamiento.
El derecho a la portabilidad de los datos, permite al presentador solicitar que se le faciliten los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

En respuesta a una solicitud de ejercicio de los derechos de protección de datos la entidad local deberá hacer constar si los datos están siendo tratados por la entidad local como responsable del tratamiento y el origen de los citados datos.
En el caso de que la entidad local no disponga de datos sobre la persona solicitante deberá hacerlo constar en la contestación y si la Entidad quiere denegar el acceso deberá establecer el motivo por el cual deniegan la solicitud (infundado o excesivo) y la información sobre el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos y de ejercitar acciones judiciales ante la denegación de la información.

VII.- IDENTIFICACIÓN INTERESADOS

1.- Publicación actos administrativos

La LOPDGDD incluye en el apartado 1º de su Disposición Adicional 7ª cómo debe identificarse a los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos, estableciendo lo siguiente**;**

"1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente."

Previamente, esta identificación incluía el nombre, apellidos y número íntegro del DNI o documento análogo; sin embargo, para minimizar el impacto en la privacidad de los ciudadanos se debe publicar el nombre, apellidos y cuatro cifras aleatorias del documento oficial de identidad.

Las Autoridades de protección de datos publican las siguientes orientaciones[13] con el fin de facilitar un criterio práctico que permita conciliar la publicación de actos administrativos con la protección de datos:

"La publicación de documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente podrá realizarse de la siguiente forma:

*• Dado un DNI con formato 12345678X, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.*

*• Dado un NIE con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, evitando el primer carácter alfabéticos, cuarta, quinta, sexta y séptima. En el ejemplo: ****4567*.*

*• Dado un pasaporte con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: *****3456.*

*• Dado otro tipo de identificación, siempre que esa identificación contenga al menos 7 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima. Por ejemplo, en el caso de una identificación como: XY12345678AB, la publicación sería: *****4567****

• Si ese tipo de identificación es distinto de un pasaporte y tiene menos de 7 dígitos numéricos, se numerarán todos los caracteres, alfabéticos incluidos, con el mismo procedimiento anterior y

13 AEPD "*ORIENTACIÓN PARA LA APLICACIÓN PROVISIONAL DE LA DISPOSICIÓN ADICIONAL SÉPTIMA DE LA LOPDGDD*" Disponible en: https://www.aepd.es/media/docs/orientaciones-da7.pdf

*se seleccionarán aquellos que ocupen las cuatro últimas posiciones. Por ejemplo, en el caso de una identificación como: ABCD123XY, la publicación sería: *****23XY.*

Los caracteres alfabéticos, y aquellos numéricos no seleccionados para su publicación, se sustituirán por un asterisco por cada posición."

El criterio provisional propuesto pretende, tratar de evitar que la adopción de fórmulas distintas en aplicación de la citada disposición pueda dar lugar a la publicación de cifras numéricas de los documentos identificativos en posiciones distintas en cada caso, posibilitando la recomposición íntegra de dichos documentos y por ello recomiendan que la fórmula propuesta sea aplicada de forma generalizada.

2.- Notificaciones con datos personales

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), establece en su artículo 40.5 lo siguiente;

"5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado."

La práctica en papel de las notificaciones normalmente se cursa a través de correos con acuse de recibo y para ello se cubre el impreso correspondiente que ha de servir de justificante de la notificación con los datos del interesado. Siguiendo el principio de minimización que establece que los datos han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, es suficiente hacer constar el nombre completo.

Lo mismo aplica para el caso de las notificaciones infructuosas reguladas en el artículo 44 de la LPACAP, por lo que en ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, salvo que esté previsto por Ley.

3.- Inclusión de los datos del denunciante en las notificaciones de denuncia.

El RGPD contiene el principio de la protección de datos por defecto. La protección de datos por defecto estriba en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento.

Teniendo en cuenta que la denuncia contiene datos personales del denunciante – incluyendo nombre y apellidos -, debe tomarse en consideración el principio de protección de datos por defecto, en la comunicación por transmisión de los datos de la denuncia al denunciado, notificando aquellos datos que sean estrictamente necesarios para el ejercicio de los derechos del interesado.

La omisión de los datos de carácter personal del denunciante en la notificación de la denuncia no supone un impedimento para el ejercicio de los derechos, ya que el denunciado podrá presentar las alegaciones, escritos y recursos que se deriven del procedimiento sancionador sin necesidad de conocer la identidad del denunciante .

VIII.- CONTRATACIÓN PÚBLICA

La protección de datos en la contratación pública tiene dos vertientes: La primera en referencia a los posibles datos de las personas involucradas en la tramitación de un procedimiento de contratación administrativa y la segunda al respecto de los datos personales tratados por los adjudicatarios durante la ejecución de los contratos.

Al respecto de la primera vertiente, CONCEPCIÓN OBISPO[14] hace referencia a la Sentencia del Tribunal Supremo de 18 de julio, concretamente la STS 1007/2019, y establece que *"ha sido quien ha dado el primer paso al respecto y ha establecido que la difusión de datos personales en abierto, es decir, con acceso ilimitado, en una página web de la Administración Pública con ocasión de la tramitación de un procedimiento de contratación administrativa está sometida al cumplimiento de las obligaciones establecidas en Ley Orgánica de Protección de Datos, y, específicamente, al deber jurídico de tener que recabar el consentimiento de los afectados sobre la recogida y tratamiento de datos cuanto no se revelen imprescindibles, necesarios o pertinentes para el adecuado y regular ejercicio de las funciones públicas, sin que quepa alegar la excepción al consentimiento de los interesados por el ejercicio de un poder o función pública."*

Sin embargo la segunda vertiente plantea nuevas problemáticas que trataremos en los puntos siguientes: La diferenciación entre encargados y corresponsables y los actos jurídicos necesarios para delimitar las obligaciones de cada uno de los implicados en el tratamiento de datos personales.

1.- Problemática diferenciación entre encargados y corresponsables

El artículo 26 RGPD crea una nueva figura, el corresponsable de tratamiento. *"Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos"*

Y tal y como concretábamos al inicio del presente trabajo:

14 Aranzadi digital num. 1/2019.CONCEPCIÓN OBISPO, T. (2019) *La contratación pública tampoco se escapa de la protección de datos.*

- Las diputaciones provinciales, consejos y cabildos insulares, serán responsables de sus respectivos tratamientos, es decir, sobre aquellos sobre los que decidan los fines de los mismos
- Respecto a aquellos tratamientos de datos derivados de la prestación de asistencia en favor de los municipios, serán encargados de tratamiento.

Al respecto de la problemática para diferenciar entre encargado y corresponsables podemos acudir al Dictamen 1/2010 del Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, ya en 2010, mucho antes de la publicación del nuevo RGPD en la que intentaba de distinguir entre responsable y encargado. En dicho texto[15] encontramos las siguientes ideas que nos pueden servir de guía para diferenciar correctamente las dos figuras:

- Es recomendable preguntarse por qué se realiza el tratamiento. ¿La otra parte lo habría realizado de no habérselo pedido el responsable? Si la respuesta es no, probablemente estemos ante un encargado, no ante un corresponsable.
- Aunque una parte "determine medios" tales como el hardware o el software que se use en el tratamiento, eso no la convierte automáticamente en corresponsable. Lo que importa son los elementos esenciales, quien determine eso será responsable/corresponsable.
- El hecho de que varios sujetos colaboren al tratar datos no significa que sean siempre corresponsables. Si los distintos tratamientos no comparten propósitos, por ejemplo, puede que la comunicación de datos entre sujetos sea únicamente una transferencia de esos datos llevada a cabo entre responsables diferenciados.
- El elemento más importante para determinar que alguien es encargado es lo de "por cuenta del responsable del tratamiento". Si alguien está obligado a seguir ese mandato, será encargado del tratamiento. Si puede determinar aspectos por sí mismo, será corresponsable.

Lo expuesto es determinante para definir que modificaciones son necesarias en la documentación de contratación pública ya que en la mayoría de las situaciones no está correctamente definida la relación con la responsabilidad en protección de datos y es necesario tener claro cual es, para saber que información se debe incluir en los contratos vigentes y futuros.

2.- Contrato de encargado

Al respecto de los tratamientos en los que la entidad local actúa como encargada del tratamiento, deberán regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

La AEPD ha publicado un documento llamado "*Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*" en el cual se establece un modelo orientativo de

15 Grupo del artículo 29 sobre protección de datos "*Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»* " Disponible en: https://sontusdatos.org/wp-content/uploads/2013/04/ce-dictamen-1-2010-conceptos-responsable-del-tratamiento-y-encargado.pdf

cláusulas para que los diferentes responsables puedan adaptarlo a las necesidades derivadas de su propia organización.

A. Modificaciones en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

La publicación del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en la materia de administración digital, contratación del sector público y telecomunicaciones, incluye modificaciones en la Ley de contratos del sector público en la materia de protección de datos que hace recomendable una revisión de las cláusulas que publica la AEPD ya que actualmente ya no se ajustan a la normativa.

El Real Decreto-ley 14/2019, de 31 de octubre, incluye las siguientes modificaciones en relación a la protección de datos:

A.1.- Modificaciones para todos los contratos

Introduce la obligación de incluir en el documento de formalización del contrato, la expresa mención al sometimiento a la normativa nacional y de la Unión Europea en la materia de protección de datos.

Introduce como causa de nulidad de pleno derecho la omisión en los pliegos de las obligaciones del futuro contratista en materia de protección de datos a los que se refiere el nuevo ar6culo 122.2 de la Ley 9/2017 de 8 de noviembre, de Contratos del sector público.

Los pliegos deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en la materia de protección de datos.

A.2.- Modificaciones para aquellos contratos en los que la ejecución requiera dela cesión de datos por parte de entidades del sector público a los contratistas

El órgano de contratación deberá especificar en el expediente de contratación cual será la finalidad del tratamiento de los datos que vayan a ser cedidos.

Será obligatorio establecer una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en la materia de protección de datos y debe advertirse de que esta obligación tiene carácter de obligación contractual esencial.

En los pliegos deberán constar las siguientes obligaciones esenciales:

a. Utilizar los datos personales objeto de tratamiento únicamente para la finalidad objeto de este contrato.

b. Cumplir en todas las fases de desarrollo del contrato, en su terminación y con posterioridad a la misma, la normativa nacional y de la Unión Europea en la materia de protección de datos, siendo responsable de cualquier infracción de la misma.
c. Presentar antes de la formalización del contrato una declaración en la que se ponga de manifiesto donde van a estar ubicados los servidores y desde donde se van a prestar los servicios asociados a los mismos.
d. Comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior
e. Indicar en su oferta si han previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por la referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

B. Cláusulas específicas

El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.

Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

La inclusión del plazo máximo por el que puedan derivarse responsabilidades de la ejecución de la prestación debe hacerse teniendo en cuenta aquellas responsabilidades en las que pueda incurrir el adjudicatario respecto de otras partes además de la Administración. Por ejemplo en la contratación de servicios, podrán derivarse responsabilidades contra los usuarios del mismo.

Puede ser recomendable, cuando se traten por el adjudicatario categorías especiales de datos, exigir un certificado de la destrucción confidencial de datos. Actualmente existen empresas, que prestan el servicio de destrucción de papel de forma segura. Esa empresa especializada en destrucción de documentos deberá garantizar la seguridad del proceso a través de un certificado, que asegurará la confidencialidad de la información a lo largo de todo el procedimiento.

En lo referente a la certificación actualmente conviven la norma UNE EN 15713:2010 del Comité Europeo de Normalización (CEN), que crea el manual de buenas prácticas para la destrucción segura de documentación en cualquier tipo de soporte y garantiza la confidencialidad y seguridad de los procesos, desde la recogida del soporte, transporte, almacenamiento de datos, destrucción y disposición final y la norma DIN 66399 del Comité de Estándares de Tecnologías de la Información y Aplicaciones (NIA) que describe los requisitos para las máquinas destructoras y procesos para la trituración de datos. El DIN realiza las mismas funciones que organismos internacionales como el

ISO, por tal motivo DIN 66399 y UNE-EN 15713 pretenden la misma finalidad y no contravienen el objetivo último que no es otro que la destrucción confidencial certificada con maquinaria industrial con un máximo nivel de seguridad.

3.- Acuerdo de corresponsabilidad

Para los tratamientos en los que la entidad local actúa como corresponsable del tratamiento, los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14.

Al respecto de la finalidad del tratamiento, si bien es cierto que la relación entre corresponsables se fundamenta habitualmente en una finalidad común, pueden coexistir fines concretos que solamente serán llevados a cabo por una de las entidades implicadas y es importante delimitarlas previamente a la ejecución del tratamiento.

El acuerdo de corresponsabilidad debe delimitar que ocurrirá con los datos objeto de tratamiento tras la finalización de la ejecución de la prestación de la que deriva el acuerdo. A pesar de que la información deba ser conservada en los plazos que la legislación determine, mientras puedan derivarse responsabilidades, puede ser que una de las partes del acuerdo cuente con medidas de seguridad implantadas de mejor calidad que la otra y le interese hacerse responsable del mantenimiento de la información para evitar posibles brechas de seguridad.

Será obligatorio que los corresponsables lleven un registro de todas las categorías de actividades de tratamiento efectuadas en el ámbito de su relación y su prestación de servicios, que contendrá lo establecido en el artículo 30 del RGPD.

Puede aprovecharse la firma de un acuerdo de corresponsabilidad para asegurar la implementación de unas medidas de seguridad extra como las siguientes:

I. Sobre el deber de confidencialidad y secreto

- Se evitará el acceso de personas no autorizadas a los datos personales, y dejar los datos personales expuestos a terceros. Cuando cualquier persona se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las veinticuatro horas del día.
- No se desecharán documentos o soportes electrónicos (CDs, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
- No se comunicarán datos personales o cualquier información personal a terceros.
- El deber de secreto y confidencialidad persistirá incluso cuando finalice la relación laboral o funcionarial del trabajador con la entidad.

II. Sobre la identificación de las personas que tratan datos personales

- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se garantizará la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas de la persona usuaria.

Debe figurar que los corresponsables se asistirán mutuamente, en la respuesta al ejercicio de los derechos que la legislación determina (acceso, rectificación, supresión y oposición; limitación del tratamiento; portabilidad de datos etc.) ya que las personas afectadas podrán dirigirse ante cualquiera de ellos.

Al respecto de las violaciones de seguridad y la gestión de riesgos es interesante tener en cuenta la capacidad de respuesta de cada entidad en cuestión, normalmente aquellas entidades de mayor tamaño tienen implantados procedimientos de gestión de brechas de seguridad o de notificación de las mismas y puede ser recomendable que sean las encargadas de gestionar las violaciones de seguridad o los riesgos que puedan afectar al tratamiento de los datos personales afectados por el acuerdo. En el caso de la gestión de seguridad, de ella se deberá derivar en todo caso la implantación de mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d) Seudonimizar y cifrar los datos personales, en su caso.

Las partes firmantes deberán designar un punto de contacto, sin perjuicio de que las personas afectadas puedan ejercer sus derechos ante cualquiera de los responsables.

Deberá figurar que el incumplimiento por parte de cualquiera de las partes de las obligaciones referidas en el acuerdo es extensible a ambas en su justa responsabilidad, respondiendo ante las Autoridades de Protección de Datos, o ante cualquier tercera persona de las infracciones que se puedan haber cometido derivadas de la ejecución del acuerdo y/o del cumplimiento de la legislación vigente en materia de protección de datos de carácter personal.

IX.- GESTIÓN DE RIESGOS

1.- Análisis de riesgos

Otro de los nuevos requerimientos que establece el RGPD para responsables y encargados del tratamiento que realizan actividades de tratamiento con datos personales es la necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información con el fin de establecer las medidas de seguridad y control orientadas a cumplir los principios de protección desde el diseño y por defecto que garanticen los derechos y libertades de las personas.

Tal y como establece la AEPD en su guía práctica de "*Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*"[16] *Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice. El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre el interesado o, por el contrario, un impacto sería significativo si el daño ocasionado sobre los derechos y libertades del interesado fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente."*

Por lo tanto, el análisis de riesgos es obligatorio en todo caso para cualquier entidad local.

La Autoridad Catalana de Protección de datos ha publicado una guía práctica[17] para la realización de una evaluación de riesgos inicial e incluye un índice de contenidos del informe de gestión de riesgos, que se transcribe a continuación:

1. Breve contextualización del proyecto
2. Objeto y alcance de la gestión de riesgos que se ha hecho
3. Metodología de gestión de riesgos que se ha utilizado
4. Potenciales escenarios de riesgo
    4.1 Medidas previstas inicialmente
    4.2 Estimación del nivel de riesgo inicial
    4.3 Medidas propuestas para tratar el riesgo inicial
    4.4 Influencia de las medidas propuestas
    4.5 Estimación del nivel de riesgo residual
5. Análisis del cumplimiento normativo y medidas para demostrar el cumplimento [si es considera la conveniencia de tratar el cumplimiento normativo aparte)
6. Conclusiones y recomendaciones

16 "*GUIA PRÁCTICA DE Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*". AEPD, 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

17 "*Guía práctica evaluación de impacto relativa a la protección de datos*". APDCAT. 2018. (Consulta 02/12/2019). Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf

2.- Evaluación de impacto

Con carácter general, hay que realizar una EIPD cuando un tratamiento puede suponer un alto riesgo para los derechos y las libertades de las personas físicas, especialmente (pero no exclusivamente), si se utilizan nuevas tecnologías y teniendo en cuenta la naturaleza, alcance, contexto o finalidades del tratamiento (considerando 76 y artículo 35.1 del RGPD).

Al contrario que en el análisis de riesgos, la evaluación de impacto sólo será necesaria en determinados casos.

La Agencia Española de Protección de Datos (AEPD) ha publicado el listado[18] de tratamientos de datos personales en los que es obligatoria la realización de una evaluación de impacto y que son los siguientes:

1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.
7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

18 AEPD "*LISTAS DE TIPOS DE TRATAMIENTOS DE DATOS QUE REQUIEREN EVALUACIÓN DE IMPACTO RELATIVA A PROTECCIÓN DE DATOS* " Disponible en: https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.
9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

A la hora de realizar una EIPD, se debe disponer de una metodología que considere los requerimientos exigidos por el RGPD en su artículo 35.7, donde se establece que la EIPD deberá incluir como mínimo: Una descripción sistemática de la actividad de tratamiento previstas, la evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad, una evaluación de los riesgos y las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

La Autoridad Catalana de Protección de datos, en su guía práctica[19] incluye un índice de contenidos del informe de evaluación de impacto para la realización de una evaluación de impacto en el ámbito de las Entidades Locales, que se transcribe a continuación:

1. Identificación del proyecto
- *1.1 Nombre*
- *1.2 Descripción breve*
- *1.3 Responsables del proyecto y datos de contacto*
- *1.4 Equipo de evaluación (quién ha hecho la evaluación de impacto)*
- *1.5 Fecha del informe*
- *1.6 Versión del informe*

2. Resumen ejecutivo
- *2.1 Descripción ejecutiva del proyecto*
- *2.2 Descripción del método de evaluación (descripción breve de cómo se ha hecho la evaluación, calendario, etapas, etc.)*
- *2.3 Principales riesgos que se han identificado*
- *2.4 Resumen de las medidas más relevantes que se han propuesto para mitigar los riesgos*

19 "*Guía práctica evaluación de impacto relativa a la protección de datos*". APDCAT. 2018. (Consulta 02/12/2019). Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf

2.5 Medidas que afectan los encargados de tratamiento.

2.6 Necesidad de hacer una consulta previa

3. Análisis de la necesidad de la evaluación (se tiene que trasladar el análisis de necesidad que se ha realizado)

3.1 Resultado del análisis

3.2 Motivación de la necesidad de hacer la EIPD

4. Descripción detallada del proyecto (se tienen que trasladar los contenidos del informe de descripción sistemática del tratamiento)

4.1 Descripción del tratamiento

4.2 Descripción detallada

4.3 Necesidad y proporcionalidad de las operaciones de tratamiento

5. Resultado del proceso de consultas (si procede)

5.1 Identificación de las partes interesadas (internas y externas).

5.2 Mecanismo de consulta y contribuciones de las partes

5.3 Resumen de los aspectos más relevantes derivados de la consulta

6. Identificación y gestión de riesgos (se tienen que trasladar los contenidos del informe de gestión de riesgos)

6.1 Identificación detallada de riesgos

6.2 Impacto y probabilidad de cada riesgo identificado

6.3 Gestión de los riesgos

6.4 Análisis de cumplimiento normativo (si es relevante, hay que segregarlo de la gestión de riesgos y deben añadirse las medidas orientadas a demostrar el cumplimiento71)

7. Conclusiones

7.1 Análisis final

7.2 Recomendaciones

7.3 Resumen de medidas a implantar

8. Anexos

8.1 Proceso de implantación de las medidas propuestas

I. Organización II. Verificación III. Monitorización

8.2 Revisión de la evaluación de impacto

I. Ordinaria II. Extraordinaria 8.3 Conceptos y definiciones.

3.- Gestión de brechas de seguridad

Se considera violación de seguridad de los datos personales toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos. Las violaciones de seguridad de los datos, más comúnmente conocidas como brechas de seguridad, se encuentran definidas en el RGPD de una forma muy amplia, de forma que incluyen todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales.

Tal y como establece el considerando 85 del RGPD "*Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos*

personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas"

La AEPD en su guía[20] para la *Gestión y notificación de brechas de seguridad* establece que "*en la medida en que la organización esté preparada para afrontar la gestión de un incidente de seguridad permitirá a la organización responder de forma rápida, ordenada y eficaz al evento, minimizando las consecuencias del mismo sobre la propia organización y terceras partes implicadas"*

Para una buena gestión de brechas de seguridad, la entidad local como responsable debe documentar las brechas de seguridad en el registro de incidencias de la Entidad y elaborar un procedimiento de respuesta a incidentes.

A. Protocolo de respuesta a incidentes

El procedimiento de respuesta a incidentes deberá contemplar lo siguiente:

- El personal de la entidad local que va a intervenir
- Las fases del procedimiento que permitan al personal que detecte una brecha de seguridad saber como tiene que actuar y que información debe recabar.
- Información concreta sobre la brecha de seguridad:
    - · Fecha y hora en la que se detecta.
    - · Fecha y hora en la que se produce el incidente y su duración.
    - · Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)
    - · Naturaleza y contenido de los datos personales en cuestión.
    - · Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
    - · Posibles consecuencias y efectos negativos en los afectados.
    - · Medidas técnicas y organizativas que se hayan adoptado.
    - · Categoría de los datos afectados y número de registros afectados.
    - · Categoría y número de individuos afectados.
    - · Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.
- Las medidas de contención posibles y las personas de contacto del Area informática.
- El personal encargado de procesar la notificación a la AEPD y a los afectados.

20 "*Guía para la gestión y notificación de brechas de seguridad*". AEPD. 2018. (Consulta 02/12/2019). Disponible en: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

B. Nofication de brechas de seguridad a la AEPD y a los afectados

La notificación a la AEPD deberá contener la siguiente información en todo caso:

- Datos identificativos y de contacto de:
  - · Responsable del tratamiento:
  - · Delegado de Protección de Datos:
- Indicación de si se trata de una notificación completa o parcial.
  En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.
- Información sobre la brecha de seguridad de datos personales

El encargado notificará la brecha de seguridad a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Así mismo, cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, la comunicará a los afectados sin dilación indebida.

La comunicación a los afectados deberá contener la siguiente información:

- Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Información sobre la brecha de seguridad de datos personales:
  - · Descripción general del incidente y momento en que se ha producido.
  - · Las posibles consecuencias de la brecha de la seguridad de los datos personales.
  - · Descripción de los datos e información personal afectados.
  - · Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
  - · Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

Tras la notificación, deberá hacerse constar en el "Registro de incidencias": el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

C. Excepción a la obligación de notificar

No será necesaria la notificación a la Autoridad de Control cuando se pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas. Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.

Asimismo no será necesaria la comunicación a los afectados cuando:

- · El responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de

seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.).
· El responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
· Cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo. *Ante esta situación, se realizará la notificación de manera pública a través de la página web*

X.- CONFLICTO ENTRE TRANSPARENCIA Y LA PROTECCIÓN DE DATOS

Cuando hablamos de transparencia conviene, con carácter previo, distinguir dos ámbitos diferenciados que se incluyen en la misma de conformidad con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno: la publicidad activa y al derecho de acceso a la información pública.

La publicidad activa, responde a la obligación, por parte de las Administraciones públicas y sus entidades e instituciones dependientes, de publicar de manera permanente determinada información pública exigida por la ley en sus portales de transparencia o sitios web, con el fin de garantizar la transparencia de su actividad.

El acceso a la información pública consiste en el derecho de cualquier persona a solicitar y obtener la información pública que considere de su interés, con los únicos límites que señale la ley. A este respecto, se considera información pública a los contenidos o documentos, cualquiera que sea su soporte o formato, que obren en poder de la Administración Regional y sus organismos públicos que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Dicho de otra manera, mientras que la publicidad activa comprende aquella información que ha de ser publicada de manera obligatoria y proactivamente y que debe ofrecerse sin necesidad de ser solicitada y con actualizaciones periódicas, el derecho de acceso a la información pública viene precedido de una petición por parte de un ciudadano para poder obtener la información que desea

La resolución de 1 de octubre (JUR 2019/18747 del Consejo de Transparencia y Buen Gobierno) trata sobre las peculiaridades de la confrontación entre estas dos vertientes de la transparencia, estableciendo lo siguiente:

Teniendo en cuanta lo anterior, debe también recodarse que, según criterio de este Organismo, amparado por diversos pronunciamientos judiciales, la información incluida dentro de las obligaciones de publicidad activa deben ser objeto de publicación de oficio siendo no obstante susceptible de una solicitud de información en caso de que no lo fuera.
Por ejemplo, en la Resolución R/0511 /2017 se razonaba lo siguiente:

> *"Así, y como ha indicado ya en ocasiones anteriores este Consejo de Transparencia y Buen Gobierno, en relación con la publicidad activa y el derecho de acceso si bien estamos ante una información que entraría dentro de las obligaciones de publicidad activa, debe*

recordarse que mediante una solicitud de acceso se puede solicitar la información de la que disponga algunos de los sujetos incluidos en el ámbito de aplicación de la norma (...),

Por su parte, la Sentencia de la sección séptima de la Audiencia Nacional de 3 de mayo de 2017 dictada en el recurso de apelación n° 16/2017:

" Y lo expuesto es indiferente del reconocimiento que hace la sentencia al hecho de que la mencionada información pueda obtenerse por vía de acceso directo, pues una y otra forma de obtención de información, -publicidad activa y publicidad pasiva-, previstas en la Ley en capítulos distintos no tienen por qué tener los mismos contenidos, refiriéndose, en todo caso, una y otra a los sujetos incluidos en el art.2 de dicha ley, como tampoco distingue en este sentido el legislador respecto de una y otra publicidad por el ente de que se trate"

Es decir, nos encontramos, por un lado, ante obligaciones de publicidad activa o de publicación de oficio de determinada información y, por otro lado, de la posibilidad de ejercer el derecho de acceso a la información que bien puede venir referido a información que debiera estar publicada pero no lo está, a información que ya se encuentra publicada (por lo que la resolución podría remitirse directamente a esta publicación según dispone el art. 22 3 de la LTAIBG) o a información diferente a la que debe ser objeto de publicación de oficio y que se encuadra en el concepto de información pública del art. 13 de la LTAIBG antes reproducido.

1.- La protección de datos en la publicidad activa

En la documentación que las Entidades Locales deben hacer pública pueden figurar datos personales.

En el tema que nos ocupa forzosamente debe hacerse referencia al artículo 69 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local que establece:

"1. Las Corporaciones locales facilitarán la más amplia información sobre su actividad y la participación de todos los ciudadanos en la vida local.

Por su parte, del Reglamento de Organización y Funcionamiento de las Entidades Locales, aprobado por el Real Decreto 2568/1986, de 28 de noviembre deben tenerse, al menos, a la vista, los siguientes artículos. El artículo 88, a cuyo tenor:

"1 .Serán públicas las sesiones del Pleno. No obstante podrá ser secreto el debate y la votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución Española, cuando así se acuerde por mayoría absoluta".

Y el artículo 196, de acuerdo con el cual:

"1. Los acuerdos que adopten el Pleno y la Comisión de Gobierno cuando tengan carácter decisorio, se publican y notifican en la forma prevista por la Ley. Iguales requisitos serán de aplicación a las Resoluciones del Alcalde o Presidente de la Corporación y miembros de ella que ostenten delegación".

En las actas del Pleno encontraremos datos personales tanto de miembros de miembros del Pleno, de empleados públicos como de ciudadanos, y es importante sentar las bases que rijan las posibilidades de incluir dicha información. Conviene tener en cuenta que el apartado 3 del artículo 5 de la reseñada Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, establece dentro de los "Principios generales" de la publicidad activa, el siguiente:

> ***"****3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos."*

A este respecto cabe transcribir el Informe 43/2014 del Servicio Jurídico de la Agencia Española de Protección de Datos que resulta muy clarificador:

> « *(...) la publicación en Internet de los datos contenidos en las actas de los Plenos y Juntas de Gobierno del Ayuntamiento constituye una cesión o comunicación de datos de carácter personal, definida por el artículo 3 j) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado".*
>
> *En relación con las cesiones de datos, prescribe el artículo 11.1 de la Ley Orgánica que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado", No obstante, no será necesario el consentimiento de los afectados cuando la comunicación se encuentre amparada por una norma con rango de Ley (artículo 11.2 a) o cuando se refiera a datos incorporados en fuentes accesibles al público (artículo 11.2 b).*
>
> *(...) De este modo, únicamente sería conforme con lo dispuesto en la Lopd la comunicación de datos, mediante su inclusión en Internet, cuando dichos datos se refieran a actos debatidos en el Pleno de la Corporación o a disposiciones objeto de publicación en el correspondiente Boletín Oficial, dado que únicamente en estos supuestos la cesión se encontraría amparada, respectivamente, en una norma con rango de Ley o en el hecho de que los datos se encuentran incorporados a fuentes accesibles al público.*
> *En los restantes supuestos, y sin perjuicio de lo dispuesto en otras Leyes, la publicación únicamente sería posible si se contase con el consentimiento del interesado o si los datos no pudieran en ningún caso, vincularse con el propio interesado (...)"*

Tomando en consideración este informe, la publicación a través de Internet de las actas de los plenos sólo es conforme a la normativa de protección de datos cuando no contiene datos de carácter personal, cuando dichos datos se refieren a actos debatidos en el Pleno o a disposiciones objeto de publicación en el Boletín Oficial que corresponda o salvo que esté amparado en una norma con rango legal, no así en los demás supuestos, requiriéndose el consentimiento del interesado para la publicación.

El tema de la publicación de los datos personales de los empleados públicos era un tema controvertido hasta la reciente publicación de la sentencia de 26 marzo 2019. JUR 2019\201813 de

la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección1ª) que se transcribe a continuación:

"Se trata, pues, de decidir si, en ese marco de cumplimiento de la obligación de publicidad activa en lo referente al presupuesto municipal, que incumbe al Ayuntamiento demandante, los datos personales de la plantilla, no los del puesto que ocupan, son adecuados e idóneos para ese fin y están habilitados por la norma o por el principio de transparencia. Cabe señalar que la principal diferencia entre el acceso a la información y la publicidad activa radica en que la primera se realiza mediante solicitud individualizada (artículo 17de la Ley 19/2013 (RCL 2013, 1772)*) mientras que la segunda permite el acceso generalizado a la información (artículo 5 de la misma Ley).*
(...) Del contenido de ambos documentos interesa ahora destacar su afirmación en el sentido de que los datos correspondientes al sueldo, complemento de destino y complemento específico se incluyen en los presupuestos generales, publicados oficialmente, y no están asociados a ningún empleado público concreto, pero si la información cuyo acceso se solicita permite esa identificación, contiene datos personales, por lo que son de aplicación las reglas y límites del artículo 15 de la Ley 19/2013 .

El criterio utilizado para determinar cuándo prevalece el interés público, representado por la transparencia de la información, concretada ahora en la utilización por los poderes públicos de los fondos presupuestarios, y cuándo el interés particular, derivado de la protección de datos personales, se basa en las características del puesto de trabajo de que se trata.

Así, para los puestos de mayor nivel de responsabilidad, autonomía en la toma de decisiones, provisión con cierto margen de discrecionalidad o con base en una relación de confianza, prevalece, por regla general, el interés derivado de la finalidad de la transparencia; entre ellos menciona varias categorías de empleados públicos, como los titulares de órganos directivos, personal eventual y de libre designación; frente a ellos se encuentra la información referente a los restantes empleados públicos que han accedido a sus puestos mediante los sistemas de provisión establecidos en las leyes reguladoras de la función pública, con independencia de la persona de quien dependan, en cuyo caso el objetivo de transparencia resulta insuficiente para limitar su derecho a la protección de sus datos personales, que prevalecerían sobre aquél objetivo. La misma conclusión se deduce de la regulación de la ley nacional y de la valenciana, ya que los artículos 9.1 g) y 12 y 13, respectivamente, antes citados, se refieren a las retribuciones de los altos cargos y asimilados, no a todo el personal.

En virtud de lo expuesto en la citada sentencia siempre es recomendable disociar aquellos datos personales de empleados públicos que puedan figurar en la información a publicar por la entidad local.

Al respecto de los datos personales de los miembros del Pleno, como son el nombre, apellidos y cargo del presidente y de los diputados que figuran en las actas, el artículo 15.2 de la La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, establece lo siguiente:

"2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano"

Los datos personales de los miembros del Pleno estarían incluidos en la excepción indicada en el artículo anterior.

Por otro lado, respecto de los datos personales que afecten a personas físicas, dichos datos deben ser disociados previamente a la publicación de los citado documentos. En este caso, sería de aplicación lo previsto en el art. 15.4 de la LTAIBG:

"No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas."

2.- La protección de datos en las solicitudes de acceso a la información pública

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas distingue los siguientes derechos:

1.- A conocer en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados.

2.- De acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y en el resto del Ordenamiento Jurídico.

Esta segunda manifestación es la que nos interesa pues la primera dependerá de la situación del interesado en relación con cada procedimiento administrativo. La Ley 19/2013 desarrolla el ejercicio de este derecho de acceso distinguiendo:

- Ámbito subjetivo de aplicación. Información pública, archivos y registros administrativos de las Administraciones Públicas Territoriales (Administración del Estado, Comunidades Autónomas y Locales) y Entidades de Derecho Público vinculadas o dependientes de las anteriores que ejerzan funciones administrativas.
- Ámbito objetivo. Comprende los registros y los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos finalizados en la fecha de la solicitud.

El acceso comprende tanto el acceso directo a los documentos en cuestión como el de obtener copias y certificados de los mismos. Existen materias excluidas del derecho de acceso, el artículo 14 de la Ley 19/2013 regula los límites al derecho de acceso, en aquellos supuestos en los que pueda suponer un perjuicio para:

a) La seguridad nacional.
b) La defensa.
c) Las relaciones exteriores.
d) La seguridad pública.
e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.
g) Las funciones administrativas de vigilancia, inspección y control.
h) Los intereses económicos y comerciales.
i) La política económica y monetaria.
j) El secreto profesional y la propiedad intelectual e industrial.
k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.
l) La protección del medio ambiente.

La aplicación de estos límites deberá estar siempre justificada, en función de las circunstancias de cada caso, y de acuerdo con el principio de proporcionalidad.

El artículo 15 regula los límites al derecho de acceso cuando la información solicitada contenga datos personales, del citado artículo podemos extraer las siguientes conclusiones:
- Si la información solicitada incluye categorías especiales de datos, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.
- Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos.
- En cualquier caso, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios establecidos en el citado artículo 15:

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.
c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.
d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

Sin embargo, el artículo 15 establece lo siguiente en su apartado cuarto "*No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas."* y el artículo 16 establece la posibilidad de conceder el acceso parcial a la información solicitada, en aquellos supuestos en los que los límites establecidos en el artículo 14 no afecten a la totalidad de la información.

Tal y como establece el dictamen1/2016 de la Comisión de Garantía del Derecho de Acceso a la Información Pública de Cataluña;

> *"La legislación de transparencia establece un principio general de "favor derecho de acceso", que obliga a acreditar y justificar caso por caso la concurrencia de límites oponibles a este derecho, y decidir su aplicación previa ponderación de los derechos e intereses en juego.*
> *18ª. Previamente a la ponderación, es necesario llevar a cabo un test del daño, para acreditar que el acceso solicitado supone efectivamente un perjuicio, y no meramente una simple afectación, a los derechos o intereses protegidos por el límite o límites concurrentes.*
> *19ª. Si el test del daño es positivo, hay que valorar hasta qué punto la información afectada es idónea y necesaria a los efectos de los derechos e intereses que constituyen la finalidad del acceso. Si esta valoración es positiva, hay que ponderar entre los derechos e intereses favorables y opuestos al acceso. Este ejercicio de ponderación debe atender, entre otros, los siguientes criterios:*
> *- Principio de proporcionalidad, que puede llevar al establecimiento de jerarquías entre los derechos e intereses confrontados, o valorar grados diferentes de perjuicio en función de las circunstancias del caso.*
> *- Los elementos de ponderación establecidos por el artículo 24.2 LTAIPBG"*

El acceso parcial a la información, que puede proceder previamente o como resultado de la ponderación, puede ser una solución para dar acceso a la información y, al mismo tiempo, proteger los derechos o intereses afectados.

XI.- CONCLUSIONES

I. En la esfera de actuaciones y obligaciones de las Entidades Locales nos hallamos ante grandes modificaciones que suponen el deber de asumir nuevas obligaciones.

Respecto del nombramiento del delegado de protección de datos en las entidades locales, teniendo en cuenta que le corresponde el ejercicio de funciones administrativas y, muy probablemente, de potestades públicas, es muy difícil justificar que la contratación de una entidad externa sea la solución adecuada por lo que en el ámbito de la Administración Local las funciones deben entenderse reservadas a los funcionarios al servicio de la entidad local correspondiente.

Al respecto de la creación del Registro de Actividades de Tratamiento es necesario tener en cuenta que el Registro debe dividirse por categorías de tratamientos y no por Departamentos. Esto es así porque un departamento puede tener diferentes tipos de tratamiento con bases legitimadoras diferentes y finalidades incluso opuestas.
Por ejemplo, un departamento de Servicios Sociales puede tener los siguientes tipos de tratamientos:

- Subvenciones, en el que la base legitimadora es el consentimiento que otorga el solicitante de la subvención cuando presenta la solicitud.
- Gestión del servicio de teleasistencia, en el que la base legitimadora sería que el tratamiento es necesario para el cumplimiento de una misión realizada en interés público

Por lo expuesto, será necesario separar correctamente cada tratamiento y definir de manera precisa la base o bases legitimadora de cada uno de los tratamientos realizados por la entidad local.

A pesar de que el Reglamento no establece dentro del contenido obligatorio del Registro de Actividades como responsables del tratamiento la información al respecto de aquellos posibles encargados del tratamiento (aquella persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento) es recomendable incluir una relación actualizada de los mismos para que las personas afectadas puedan conocer quien está tratando sus datos personales.

II. En lo referente al cumplimiento del deber de información es habitual que en los modelos de información facilitados por las Administraciones Públicas no figuren los datos completos del Delegado de protección de datos. Al respecto de esto el artículo 30 del RGPD es claro cuando establece que debe figurar *"el nombre y los datos de contacto del delegado de protección de datos*". Además el artículo 74.p) de la LOPDGDD considera como infracción leve *"No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica"*

Al respecto de la publicación de los datos de contacto de los posibles encargados del tratamiento, desde mi punto de vista es recomendable que las personas afectadas puedan conocer "quien" trata sus datos personales.

Para cumplir correctamente con el deber de información es importante tener clara la diferencia entre un destinatario y un encargado del tratamiento, ya que se pueden encontrar informaciones contradictorias al respecto. Para distinguirlos cabe discernir si tratará los datos por su cuenta (Destinatario) o por cuenta del Responsable (Encargado).

III. En lo referente a la forma de ejercicio de los derechos de protección de datos es recomendable utilizar aquella forma que permita a la entidad local tener constancia fehaciente de la entrada de la solicitud y que permita responder a la misma con suficiente virtualidad administrativa. Puede ser recomendable articularlo a través de la Sede Electrónica de la entidad local o de manera presencial,

presentando la solicitud firmada y por escrito en cualquiera de las oficinas o registros de los previstos en la normativa reguladora del procedimiento administrativo común para la presentación de documentos que las personas interesadas dirijan a las Administraciones públicas.

IV. En el ámbito de las Entidades Locales se tratan categorías especiales de datos personales con relativa normalidad, sobretodo datos de salud en el ámbito de los Servicios Sociales o en aquellas entidades titulares de centros educativos. Es por ello recomendable, que en el caso de que se traten categorías especiales de datos personales se recabe siempre el consentimiento expreso e inequívoco.

Teniendo en cuenta que los datos referidos a los menores gozan de una especial protección ya que su tratamiento se considera de riesgo es importante tener en cuenta la excepción que contempla la LOPDPGDD cuando establece que el tratamiento de los datos de un menor de edad no podrá fundarse en su consentimiento cuando la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento.

Esto es importante, sobretodo para aquellas Entidades Locales titulares de centros educativos, ya que tendrán que diferenciar correctamente aquellos actos o negocios jurídicos en los que la ley exija la asistencia de los titulares de la patria potestad para solicitarles el consentimiento para el tratamiento de los datos personales del menor a ellos y no al menor aunque supere los 14 años de edad.

V. Para la notificación y publicación de actos administrativos deberán tenerse en cuenta las recomendaciones publicadas por la AEPD para minimizar el impacto en la privacidad de los ciudadanos por las que se debe publicar el nombre, apellidos y cuatro cifras aleatorias del documento oficial de identidad.

A los efectos de modificar la documentación contractual de la entidad local debemos tener en cuenta que los tratamientos de las entidades locales se podrán dividir en tres tipos.

- Tratamientos en los que la entidad local actúa como responsable porque decide sobre los fines de los mismos.
- Tratamientos en los que la entidad local actúa como encargada porque está prestando un servicio al responsable del tratamiento y no decide sobre la finalidad de los datos pero si los trata por cuenta del responsable.
- Tratamientos en los que la entidad local actúa como corresponsable, normalmente con otra Administración Pública, porque ambas deciden conjuntamente los medios y finalidades del tratamiento.

La publicación del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en la materia de administración digital, contratación del sector público y telecomunicaciones, incluye modificaciones sustanciales en relación a la protección de datos que deberán ser tenidas en cuenta por el órgano de contratación al redactar los pliegos de cláusulas administrativas de los contratos.

VI. En lo referente a la gestión de riesgos es importante diferenciar que el análisis de riesgos será obligatorio en todo caso para cualquier entidad local y en cambio la evaluación de impacto sólo será necesaria cuando un tratamiento puede suponer un alto riesgo para los derechos y las libertades de las personas físicas.

Al respecto de la elaboración de un procedimiento de respuesta a incidentes, el mismo tiene su justificación en el plazo que ofrece la normativa para notificar las brechas de seguridad a la AEPD. En 72 horas si la Entidad no tiene claro que pasos debe seguir muy probablemente no llegue a notificar la incidencia en el plazo establecido.

VII. La conciliación de los preceptos de la Ley 19/2013, de 9 de diciembre, de Transparencia con la normativa de protección de datos, presenta bastantes dudas.

En lo referente a las obligaciones de publicidad activa, se entenderá justificada la incorporación de datos personales cuando dichos datos se refieren a actos debatidos en el Pleno o a disposiciones objeto de publicación en el Boletín Oficial que corresponda o que esté amparado en una norma con rango legal, no así en los demás supuestos, requiriéndose el consentimiento de los interesados para la publicación. Sin embargo los datos personales de los miembros del Pleno podrán publicarse en base a la excepción establecida en el artículo 15.2 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Por otro lado, respecto de los datos personales que afecten a personas físicas, siempre es recomendable disociar dichos datos previamente a la publicación

Para conceder el acceso a la información pública siempre es recomendable efectuar una disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectas y prevalezca el derecho a acceder a la información pública. En el caso de que esto no sea posible se deberá realizar la ponderación de los intereses y derechos en juego en el caso concreto, valorando la posibilidad de conceder el acceso parcial a la información.

BIBLIOGRAFÍA

RALLO LOMBARTE, A. (Dtor.) (2019), *Tratado de Protección de Datos, actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personables y garantía de los derechos digitales,* 1ª edición, Valencia, Tirant lo Blanch.

CAMPOS ACUÑA, C. (Dtra) (2018), *Aplicación práctica y adaptación de la protección de datos al ámbito local*, 2ª edición, Madrid, Wolters Kluwer

LÓPEZ CALVO, J. (Coord.) (2018)*, El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* 1ª edición, Madrid, BOSHH – Wolster Kluver.

ADSUARA VARELA, B. *"El Consentimiento"* en Piñar Mañas, J.L (Director). Reglamento Europeo de Protección de Datosm hacia un modelo europeo de privacidad. Reus, Madrid, 2016.

CONCEPCIÓN OBISPO, T. (2019) *La contratación pública tampoco se escapa de la protección de datos.* Aranzadi digital num. 1/2019.

ACÍN FERRER, A. (2019) *Protección de datos. Aplicación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, en las entidades locales Entidades locales.- Actuaciones y responsabilidades.* La Administración Práctica num. 2/2019.

A. MESSÍA. J (2018) *Consideraciones y perspectivas del delegado de protección de datos.* Revista Aranzadi de Derecho y Nuevas Tecnologías num. 47/2018

GONZÁLEZ CALVO M. (2018) *La nueva figura del delegado de protección de datos*. Actualidad Jurídica Aranzadi num. 939/2018.

GUÍAS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2017-2019)

1. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento

2. Guía de Privacidad desde el diseño

3. Guía de protección de datos y Administración local

4. Guía para centros educativos

5. Guía para el cumplimiento del deber de informar

6. Guía para el responsable de tratamientos de datos personales

7. Guía para la gestión y notificación de brechas de seguridad

8. Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD

9. Guía sobre el uso de videocámaras para seguridad y otras finalidades

10. Guía práctica para las evaluaciones de impacto en la protección de datos personales

11. Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas